PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-154118
(43)Date of publication of application : 09.06.1998

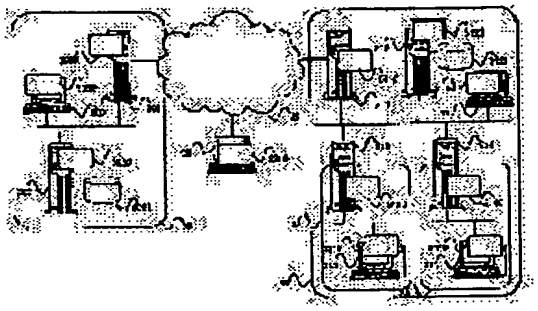
(51)Int.Cl. G06F 13/00
G06F 13/00
G06F 15/00
H04L 9/32

(21)Application number : 08-312036
(22)Date of filing : 22.11.1996

(71)Applicant : HITACHI LTD
(72)Inventor : MIYAKE SHIGERU
TEZUKA SATORU
MIYAZAKI SATOSHI
KAYASHIMA MAKOTO
KOIZUMI MINORU
KATSUMATA OSAMU

(54) NETWORK COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To enable a proper user to perform the communication between the computers having the intervention of plural fire walls with no consciousness of a communication channel by using a directory service computer.
SOLUTION: A client 303 designates a user ID, etc., and is authenticated by a directory service server 302 of a network 30. Then the client 303 designates the device name of a directory service server 312 of a network 31 and inquires about the channel information. Based on the acquired channel information. the fire wall servers 301 and 311 connect the client 303 to the server 312 via an internet 32. The client 303 is authenticated by the server 312 and then designates the device name of a server 331 to inquire about the channel information. Based on this channel information, the fire wall servers 311 and 313 decides a communication channel between the client 303 and the server 331.



LEGAL STATUS
[Date of request for examination] 10.09.1999
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－154118

(43)公開日　平成10年(1998)6月9日

(51)Int.Cl.⁶		識別記号	FI		
G06F	13/00	355	G06F	13/00	355
		357			357 Z
	15/00	330		15/00	330 C
H04L	9/32		H04L	9/00	673 B
					673 A

審査請求　未請求　請求項の数6　OL　（全10頁）

(21)出願番号　特願平8-312036

(22)出願日　平成8年(1996)11月22日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地

(72)発明者　三宅　滋
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　手塚　悟
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　宮崎　聡
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　富田　和子

最終頁に続く

(54)【発明の名称】ネットワーク通信システム

(57)【要約】

【課題】　複数のファイアウォールが介在する計算機間の接続を正当なユーザが通信経路を意識することなく容易に実施できるようにする。

【解決手段】　クライアントからサーバの接続を制限する複数のファイアウォールを有するネットワークに、ディレクトリサービスサーバを設置する。ディレクトリサービスサーバは、ネットワーク内の各計算機の識別情報、アクセス可能なユーザ、通信経路などの情報を記憶し、アクセスしてきたクライアントのユーザがサーバの正当なユーザの場合、指定されたサーバの識別情報からサーバへの通信経路の情報を検索し中継サーバに提供する。通信経路の情報を基に中継サーバはクライアントとサーバ間の通信経路を確立する。また、ディレクトリサービスサーバとファイアウォールは自計算機の設定情報を互いに通信し、他の計算機でなされた設定情報の登録・更新に応じて自計算機の設定情報の登録・更新を行う。

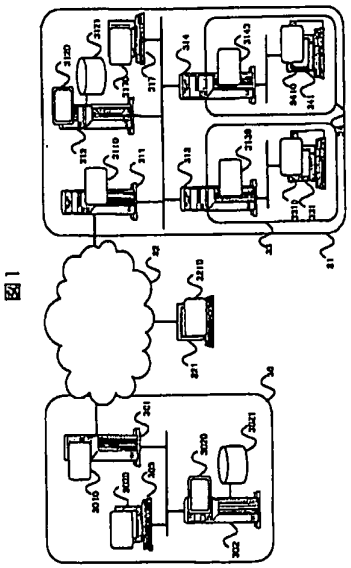


図1

1

【特許請求の範囲】

【請求項1】ネットワークを構成する、クライアント計算機と、サーバ計算機と、当該クライアント計算機およびサーバ計算機の通信の中継点に配置された、ファイアウォールの機能を有する複数の中継サーバ計算機と、ディレクトリサービス計算機とを備え、

当該ディレクトリサービス計算機は、

前記ネットワークを構成する各計算機を識別するための識別情報と、当該各計算機にアクセス可能なユーザを規定したユーザ情報と、当該各計算機の前記ネットワークにおける通信経路を規定した経路情報とが格納されたデータベースと、

前記クライアント計算機から、前記サーバ計算機の識別情報と、前記クライアント計算機のユーザを指定する情報とを受け付ける手段と、

当該受け付けた情報を基に、前記データベースに格納された識別情報およびユーザ情報を検索して、前記クライアント計算機のユーザが前記サーバ計算機の正当なユーザであるか否かを判定する判定手段と、

前記クライアント計算機のユーザが前記サーバ計算機の正当なユーザである場合、前記データベースに格納された経路情報の内の、前記中継サーバ計算機からサーバ計算機に到る通信経路を規定した経路情報を前記中継サーバ計算機へ送る手段とを有し、

前記中継サーバ計算機は、

前記ディレクトリサービス計算機から送られた経路情報で示される通信経路で前記クライアント計算機の通信を中継する手段を有することを特徴とするネットワーク通信システム。

【請求項2】請求項1記載のネットワーク通信システムであって、

前記クライアント計算機のユーザが前記サーバ計算機の正当なユーザである場合、前記各中継サーバは、前記クライアント計算機からサーバ計算機に到る通信経路を確立し、かつ、前記クライアント計算機の通信に対するファイアウォールの認証手続を免除することを特徴とするネットワーク通信システム。

【請求項3】請求項1記載のネットワーク通信システムであって、

前記ディレクトリサービス計算機も、アクセスしてきたクライアント計算機のユーザの認証を行う手段を有し、

前記判定手段は、当該認証が得られなかったユーザは正当なユーザでないと判定することを特徴とするネットワーク通信システム。

【請求項4】請求項3記載のネットワーク通信システムであって、

前記ディレクトリサービス計算機は、前記クライアント計算機のユーザが正当なユーザである場合、前記データベースに格納された、前記クライアント計算機のユーザがアクセス可能な計算機の識別情報を前記クライアント計算機に送る手段を有することを特徴とするネットワーク通信システム。

【請求項5】請求項1記載のネットワーク通信システムであって、

前記ネットワークは、前記クライアント計算機が構成する第1のネットワークと、前記サーバ計算機とディレクトリサービス計算機と複数の中継サーバ計算機が構成する第2のネットワークとにより構成されており、

前記第1および第2のネットワークの接続点には、1つの前記中継サーバ計算機が配置されることを特徴とするネットワーク通信システム。

【請求項6】請求項1記載のネットワーク通信システムであって、

前記ディレクトリサービス計算機と中継サーバ計算機は、それぞれに、

自計算機に格納されている情報に対する更新情報を受け付ける手段と、

当該更新情報を基に、前記格納されている情報を登録・更新を行う手段と、

前記格納されている情報の内、他の計算機で格納されている情報と関連する情報を、前記他の計算機との間で互いに通信する手段と、

当該通信において他の計算機から送られた情報を基に、自計算機に格納されている情報が前記他の計算機でなされた情報の更新を反映したものとなるように、前記格納されている情報を登録・更新する手段とを有することを特徴とするネットワーク通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、計算機間の通信に複数のファイアウォールが介在するネットワーク通信システムに関し、特に、計算機間の接続の管理方法に関するものである。

【0002】

【従来の技術】現在、企業間あるいは企業内の事業部間のネットワークの相互接続や、遠隔オフィス／在宅勤務の通信を、インターネットを介して行えるようにするネットワーク環境の整備が進められている。このようなネットワークでは、不正接続や通信データの盗聴等を防止し、セキュリティを確保するために、一般的にファイアウォール（防火壁）を設置している。

【0003】ファイアウォールは、例えばインターネットと企業内のネットワークの接続点のような、ネットワークの境界部分に配置され、保護対象のネットワークの構成や構成要素等の情報を、外部のネットワークから取得できないよう隠蔽する。さらに、ファイアウォールは、設定された情報を用いて、アクセス要求元のユーザの認証を行い、その結果に基づくアクセス制御により正当なユーザの通信のみを実施可能とする。

【0004】企業内のネットワークでは、例えば事業所

毎に分割したサブネットワークにファイアウォール（内部ファイアウォール）を設置して、そのサブネットワークを企業全体のネットワークから分離して保護している場合が多い。このため、企業内のネットワークの通信でも複数のファイアウォールが介在するのが一般的となっている。

【０００５】ファイアウォールの設置された企業内のネットワークのサーバへ、ネットワーク外部のクライアントからファイアウォールを越えてアクセスすることを可能とする手段として、socks_V5がRFC1928で提案されている。socks_V5では、各クライアントと中継サーバの間での相互認証と、中継サーバに対する接続命令とを実現するsocksプロトコルが定義されており、ファイアウォールを介したクライアントとサーバ間の通信を可能とする。

【０００６】また、IPレイヤにおける中継経路情報の交換を動的に行なうメカニズムとしては、RIP(Routing Information Protocol:RFC1058)、OSPF(Open Shortest PathFirst:RFC1131)等のゲートウェイプロトコルがある。

【０００７】また、ネットワークに接続しているコンピュータやネットワークを利用しているユーザ等の情報を、データベースを用いて統合的に管理する方法としては、X.500で規定されたディレクトリサービスが国際標準として利用されている。

【０００８】

【発明が解決しようとする課題】上記従来のネットワーク通信システムで、クライアントとサーバの通信に複数のファイアウォールが介在する場合、クライアントはファイアウォールによりサーバの経路情報を入手することができない。このため、サーバの通信経路が分からないユーザは、正当なユーザであっても、サーバへのアクセスを実施することができなかった。例えば、図７に示すネットワーク通信システムで、A社ネットワーク10のクライアント101が、B社ネットワーク11においてサーバ113へのアクセスを許可されており、また、B社ネットワーク11への通信経路を分かっている場合、クライアント101は、上記通信経路で外部ファイアウォールA103,B111に順次アクセスし認証を行うことでB社のネットワーク11へは接続することができる。しかし、外部ファイアウォールB111で、内部ファイアウォールC112およびサーバ113の経路情報を取得することができないため、例えばサーバ113の名称しか分からないクライアント101は、サーバ113へつながる次の接続先も分からず、サーバ113にアクセスすることができない。

【０００９】また、従来のネットワーク通信システムでは、１つのネットワークに複数のファイアウォールを設置する場合、各ファイアウォールが保護するサブネットワークへの接続の可否の決定や、クライアントの認証、アクセス制御等に用いる各種設定情報の登録や更新を、各ファイアウォール毎に個別に行う必要があった。このため、例えば或る経路の経路情報の登録や更新を行う場合、管理者はその経路上の全てのファイアウォールに対し、登録や更新の作業を繰り返さなければならなかった。例えば、図８に示すネットワーク通信システムでは、サーバ203と社外のネットワークとの接続条件等に変更が生じた場合、外部ファイアウォール201と内部ファイアウォール202の各設定を更新する必要がある。また、管理者は、外部ファイアウォール201の設定変更を外部ファイアウォール201に直接接続された設定コンソール端末A204で行い、内部ファイアウォール202の設定は別の地点に設置された設定コンソールB205で行わなければならない。

【００１０】そこで、本発明は、複数のファイアウォールが介在する計算機間の通信を正当なユーザが通信経路を意識することなく実施できるネットワーク通信システムを提供することを目的とする。さらに、そのネットワーク通信システムで行われる情報の登録・更新の作業を軽減することを目的とする。

【００１１】

【課題を解決するための手段】上記の目的を達成するため、本発明は、ネットワークを構成する、クライアント計算機と、サーバ計算機と、当該クライアント計算機およびサーバ計算機の通信の中継点に配置された、ファイアウォールの機能を有する複数の中継サーバ計算機と、ディレクトリサービス計算機とを備え、当該ディレクトリサービス計算機は、前記ネットワークを構成する各計算機を識別するための識別情報と、当該各計算機にアクセス可能なユーザを規定したユーザ情報と、当該各計算機の前記ネットワークにおける通信経路を規定した経路情報とが格納されたデータベースと、前記クライアント計算機から、前記サーバ計算機の識別情報と、前記クライアント計算機のユーザを指定する情報とを受け付ける手段と、当該受け付けた情報を基に、前記データベースに格納された識別情報およびユーザ情報を検索して、前記クライアント計算機のユーザが前記サーバ計算機の正当なユーザであるか否かを判定する判定手段と、前記クライアント計算機のユーザが前記サーバ計算機の正当なユーザである場合、前記データベースに格納された経路情報の内の、前記中継サーバ計算機からサーバ計算機に到る通信経路を規定した経路情報を前記中継サーバ計算機へ送る手段とを有し、前記中継サーバ計算機は、前記ディレクトリサービス計算機から送られた経路情報で示される通信経路で前記クライアント計算機の通信を中継する手段を有することを特徴とするネットワーク通信システムを提供する。

【００１２】このネットワーク通信システムでは、クライアント計算機のユーザがアクセス対象のサーバ計算機の正当なユーザである場合、ディレクトリサービス計算機がサーバの識別情報（例えば、サーバの装置名称やアドレス）を基にデータベースを検索してクライアント計算機とサーバ計算機間の経路情報を中継サーバ計算機へ送り、その経路情報を用いて中継サーバ計算機がクライアント計算機の通信を中継する。これにより、クライアント計算機のユーザは、通信経路を意識することなくサーバ計算機との通信を実施することができる。

【００１３】また、本発明は、前述のネットワーク通信システムであって、前記ディレクトリサービス計算機と中継サーバ計算機とファイアウォール計算機は、それぞれに、自計算機に格納されている情報に対する更新情報を受け付ける手段と、当該更新情報を基に、前記格納されている情報を登録・更新を行う手段と、前記格納されている情報の内、他の計算機で格納されている情報と関連する情報を、前記他の計算機との間で互いに通信する手段と、当該通信において他の計算機から送られた情報を基に、自計算機に格納されている情報が前記他の計算機でなされた情報の更新を反映したものとなるように、前記格納されている情報を登録・更新する手段とを有することを特徴とするネットワーク通信システムを提供する。

【００１４】このネットワーク通信システムでは、前記ディレクトリサービス計算機と中継サーバ計算機とファイアウォール計算機において、１つの計算機に格納されている情報になされた登録・更新が、他の全ての計算機に格納されている情報に自動的に反映される。このため、管理者が情報の登録・更新を各計算機について個別に行わずに済み、情報の登録・更新の作業は軽減される。

【００１５】

【発明の実施の形態】本発明の実施の形態を、図１から図６を用いて説明する。

【００１６】図１は、本発明の実施形態に係るネットワーク通信システムの構成を、仮想ネットワークとして示した図である。図１のネットワークでは、ネットワーク30とネットワークA31がインターネット32により接続されている。ネットワーク30には、ファイアウォール・サーバ301と、ディレクトリサービス・サーバ302と、クライアント303とが含まれる。ネットワークA31には、ファイアウォール・サーバ311,313,314、ディレクトリサービス・サーバ312、サーバ331,341、クライアント303が含まれ、サーバ313,331と、サーバ314,341は、それぞれサブネットワークB31,C34を構成している。さらに、インターネットにはクライアント321が直接接続されている。

【００１７】ファイアウォール・サーバ301,311,313,314にそれぞれ設けられたプログラム3010,3110,3130,3140は、ファイアウォールの機能と中継サーバの機能を実現する。クライアントおよびサーバ3030,321,317,331,341にそれぞれ設けられたプログラム3030,3170,3210,3310,3410は、ネットワーク通信の機能と中継サーバの機能を実現する。ディレクトリサービス・サーバ302,312にそれぞれ設けられたプログラム3020,3120は、ディレクトリサービスの機能を実現する。なお、本ネットワークのファイアウォール・サーバは、ファイアウォールの機能を持った中継サーバ（代理サーバ）と定義することができる。また、ファイアウォールの機能と中継サーバの機能をそれぞれ別のサーバで実現してもよい。

【００１８】図２は、ファイアウォール・サーバと、クライアントの構成を示す図である。

【００１９】図２において、ファイアウォール・サーバおよびクライアントは、主記憶装置42、バス43、CPU44、通信I/Oインタフェースコントローラ45、キーボードマウスコントローラ46、キーボード461、ビデオボードコントローラ47、ディスプレイ装置472、ディスクコントローラ41、固定ディスク装置410により構成される。固定ディスク装置410には、ネットワーク通信を可能とする通信プログラム411と、上記ネットワーク通信を、指定された通信経路で行うためのデータ中継制御プログラム412と、経路情報等の更新処理を行うためのディレクトリ情報同期プログラム413と、通信経路の決定に利用する経路情報の設定された中継経路テーブル414とが予め格納されている。ここで、経路情報は、自計算機の中継経路に含まれる計算機のアドレスの対応関係を示す情報である。主記憶装置42には、中継経路テーブルの情報等が格納されるデータ中継経路情報記憶領域421と、通信データ記憶領域422と、ディレクトリ同期情報記憶領域423と、プログラムロード領域424とが形成されている。固定ディスク装置410の各プログラムは、プログラムロード領域424に転送された後、CPU44により実行される。なお、ファイアウォール・サーバの固定ディスク装置410には、クライアントおよびそのユーザの認証を可能とする認証プログラムおよび認証情報（図示略）も格納されている。

【００２０】図３は、ディレクトリサービス・サーバの構成を示す図である。

【００２１】図３において、ディレクトリサービス・サーバは、主記憶装置52、バス53、CPU54、通信I/Oインタフェースコントローラ55、キーボードマウスコントローラ56、キーボード561、ビデオボードコントローラ57、ディスプレイ装置572、ディスクコントローラ51、固定ディスク装置510により構成される。固定ディスク装置510には、通信プログラム511と、ディレクトリデータベース制御プログラム512と、ディレクトリ情報同期プログラム513と、ディレクトリデータベース514と、クライアントおよびそのユーザの認証を可能とする認証プログラムおよび認証情報（図示略）が予め格納されている。

【００２２】主記憶装置52には、ディレクトリデータ記憶領域521と、ディレクトリ同期情報記憶領域522と、プログラムロード領域523とが形成されている。ディレクトリデータベース514には、管理対象のネットワークの

全ての経路情報が設定された中継経路テーブルの他に、オブジェクト情報テーブルと、属性情報テーブルが形成されている。これらの各テーブルの情報は、ネットワーク管理者により一括して登録および更新される。

【0023】図4に、ディレクトリデータベース3121の登録内容の概要を示す。図4中のシンボル60～631の各々は、ディレクトリサービス・サーバが管理するネットワークA31の各種機器やユーザ等を表している。シンボル60は外部ネットワークのあるディレクトリのRootオブジェクト、シンボル61はネットワークA、シンボル611はネットワークAと外部ネットワークを中継するファイアウォール1、シンボル612は後述するファイアウォール2へのポインタとなるエイリアスオブジェクト、シンボル613はディレクトリサービスを提供するサーバ、シンボル62はネットワークA内部のサブネットワークB、シンボル621,622は規定の位置がサブネットワークBであるユーザ、シンボル623は規定の位置がサブネットワークBであるユーザが所属するグループ、シンボル624はサブネットワークBに配置された内部ファイアウォール、シンボル625はサブネットワークBに配置されたサーバ、シンボル63はサブネットワークC、シンボル631は規定の位置がサブネットワークCであるユーザを、それぞれ示す。

【0024】図4に示すように、ディレクトリデータベースの登録情報は、ネットワークの構成をディレクトリツリーと呼ばれる木構造の図で表現することができる。ネットワーク上の各オブジェクトの配置は、ディレクトリツリーでRootからそのオブジェクトに到達するまでに通過するオブジェクトにより特定される。通過するオブジェクトの列により表される階層的な配置のことをコンテキストと呼ぶ。なお、各オブジェクトを実ネットワークの接続状況と同様に配置して、そのコンテキストにより実ネットワーク上の配置を表すこともできる。

【0025】図5は、ディレクトリデータベース3121に形成されたオブジェクト情報テーブルの一例である。オブジェクト情報テーブルには、管理対象のネットワークのディレクトリツリーの情報が登録される。図5において、オブジェクト情報テーブルは、図4のディレクトリの各オブジェクト毎に、オブジェクトを識別するためのオブジェクトID701、オブジェクト名702と、ディレクトリツリー上の位置（通過するオブジェクト）を示すコンテキスト703と、オブジェクト型704と、後述の属性情報テーブルへの識別子となる属性ID705とが登録される。オブジェクトを識別するための情報に、ネットワークや計算機のアドレスを含めてもよい。ディレクトリデータベースでは、オブジェクトID701を基に処理・制御が行われる。なお、このオブジェクト情報テーブルに、シンボルのイメージデータを付加して、図4のようなディレクトリツリーのグラフィック表示を行えるようにしてもよい。ただし、このサービスをクライアントに提供する場合は、そのユーザがアクセス可能な部分のみを表示できるようにする。さらに、誤りの検出・訂正を可能とする冗長データを付加してもよい。

【0026】図6は、ディレクトリデータベース3121に形成される属性情報テーブルの一例である。属性情報テーブルには、ディレクトリツリーの各オブジェクトの詳細な属性が設定される。図6において、属性情報テーブルには、オブジェクト情報テーブルから参照される際の識別子となる属性ID801と、同一属性IDの各詳細属性を識別するための補助ID802と、オブジェクト属性の種類を示す名前803と、同一名のオブジェクト属性を区別するためのシリアル番号804と、アクセス権限等を規定する属性の設定値805とが登録される。例えば、図6中の属性812は、ユーザ1がファイアウォール1に対するデータの読み出しと書き込みが可能であることを表している。属性826は、ファイアウォール2を介した全ての経路での通信をユーザ1に許可することを表している。属性828は、規定の位置がネットワークAに無いユーザProject User.Externalに、ファイアウォール2を介する経路Route.0での通信を許可することを表している。本例では、ProjectUser.Externalに、ファイアウォール1へのアクセス権限(814)と、ファイアウォール2に対するアクセス権限(819)と、ディレクトリサービスへのアクセス権限(824)を与えている。

【0027】本ネットワーク通信システムで行われる情報更新処理を説明する。

【0028】ディレクトリサービス・サーバと、中継サーバの機能を持つ各ファイアウォール・サーバは、ディレクトリ情報同期プログラム512を実行して、定期的に自計算機の設定情報（経路情報など）を交換し合い、設定情報の登録・更新を行う。この処理により、例えば、ディレクトリサービス・サーバとファイアウォール・サーバにそれぞれ格納された同一経路についての経路情報が一致しない場合は、設定日時の新しい経路情報に統一するように中継経路テーブルの経路情報が更新される。接続の可否の決定やクライアントの認証等に用いる情報も、同様にして登録・更新される。また、インターネットを介して互いに接続されたネットワーク30,31の外部ファイアウォールも設定情報を互いに交換し、自ネットワークへのアクセスを許可するユーザの情報の登録・更新を行う。例えば、ネットワーク31において、ネットワーク30のユーザの自ネットワーク31へのアクセスを許可する登録を行った場合には、同内容の登録がネットワーク30のディレクトリサービス・サーバとファイアウォール・サーバにもなされる。このように、本ネットワーク通信システムでは、ネットワーク管理者は各計算機の設定情報の登録・更新を、例えばディレクトリサービス・サーバでのみ実施すればよく、従来のシステムのように各ファイアウォール・サーバ毎に個別に登録・更新を実施しなくてもよい。

【0029】次に、本ネットワーク通信システムにおける通信動作の具体例を説明する。

【0030】まず、図1において、ネットワークB33のサーバ331へのアクセス権を与えられたユーザが、そのサーバ331に、他のネットワーク30内のクライアント303からアクセスする場合を説明する。

【0031】ユーザからネットワークA31へのアクセスを指示されたクライアント303は、まず、自クライアントのMACアドレスやユーザ名称、ユーザID等を指定してネットワーク30内のディレクトリサービス・サーバ302の認証を受ける。そして、クライアント303は、ディレクトリサービス・サーバ302に、ネットワークA31内のディレクトリサービス・サーバ312の識別情報（例えば装置名称）を指定して経路情報を問い合わせ、経路情報を取得する。なお、このとき、ネットワーク30内のファイアウォール・サーバ301とディレクトリサービス・サーバ303には、情報更新処理等により上記ユーザのネットワークA31へのアクセスを許可する設定がなされている。取得した経路情報に従いクライアント303、ファイアウォール・サーバ301、ネットワークA31のファイアウォール・サーバ311は、各中継サーバプログラムにより、クライアント303をインターネット32を介してディレクトリサービス・サーバ312に接続する。

【0032】そして、クライアント303は、ディレクトリサービス・サーバ312との間で上記と同様の認証手続を行った後、サーバ331の装置名称を指定してディレクトリサービス・サーバ312に経路情報を問い合わせる。問い合わせに対しディレクトリサービス・サーバ312は、上記ユーザのサーバ331へのアクセスが許可されているため、サーバ331への経路情報を返送する。この経路情報に従いファイアウォール・サーバ311,313は、中継サーバプログラムによりクライアント303とサーバ331間の通信経路を確立し、その通信経路におけるクライアント303の認証手続は免除する。以降、クライアント303はサーバ331と通信し、サーバ331の資源を利用することができる。

【0033】次に、規定の位置がサブネットワークB33でサーバ331へのアクセスを許可されたユーザ（図6のユーザ1）が、インターネット上のクライアント321から、サーバ331にアクセスする場合を説明する。このユーザは、ネットワークA内のディレクトリサービス・サーバ312とサーバ331の装置名称を知っているものとする。

【0034】サーバ331へのアクセスが指示されるとクライアント321は、中継サーバプログラムにより、ファイアウォール311で認証を得てディレクトリサービス・サーバ312に接続する。そして、ディレクトリサービス・サーバ312でユーザID等の指定によりユーザの認証を受けて、サーバ3310への経路情報をディレクトリサービス・サーバ312に要求する。この要求を受けたディレクトリサービス・サーバは、ディレクトリデータベース制御プログラムにより、サーバ331に対応するオブジェクトをディレクトリデータベース3121で検索し、ユーザ1のアクセス権利822が読み書き可能なrwの値となっていることを確認し、次に途中経路にあるファイアウォール2へのルートの使用権限826があることを確認し、サーバ331へのルートの使用権限があることを確認した後、クライアント321からサーバ331に到る通信経路の経路情報を返送する。この経路情報に従いファイアウォール・サーバ311とファイアウォール・サーバ313は、各中継サーバプログラムにより通信経路を確立し、クライアント321に対する認証手続は免除する。そして、以降、クライアント321とサーバ331の間の通信を中継する。

【0035】以上のように、本ネットワークでは、正当なユーザは通信経路を意識することなしに目的のサーバとの通信を容易に実施することができる。

【0036】なお、ファイアウォール・サーバでの通信経路の確立と認証手続の免除を行わずに、クライアントに経路情報のみを提供するようにしてもよい。この場合、クライアントは、提供された経路情報を基に中継経路上のファイアウォール・サーバに順次にアクセスし認証手続きを行って、サーバ331との間の通信経路を確立する。また、経路情報の変わりに上記のコンテキストをクライアントに提供し、コンテキストを基にサーバ331との間の通信経路を確立するようにしてもよい。

【0037】また、例えばProjectUser.Externalとして、ファイアウォール1へのアクセス権限814、ファイアウォール2に対するアクセス権限819およびディレクトリサービスへのアクセス権限824を許可されたユーザは、規定の位置がネットワークAに無い場合にも外部からサーバ331にアクセスできる。また、ディレクトリサービス・サーバへのアクセス権限を不許可としておけば、仮にファイアウォール1へ不正アクセスしたユーザがいたとしても、ディレクトリサービス・サーバ312との認証を行うことが必要となるため、ネットワークA内部への不正アクセスを阻止し、セキュリティを確保することができる。

【0038】

【発明の効果】以上のように、本発明によれば、複数のファイアウォールが介在する計算機間の通信を正当なユーザが通信経路を意識することなく容易に実施できるネットワーク通信システムを提供することができる。さらに、そのネットワーク通信システムで行われる情報の登録・更新の作業を軽減することができる。

【図面の簡単な説明】

【図1】 本発明の実施形態に係る通信システムの全体構成を示す図である。

【図2】 サーバまたはクライアントの構成を示す図である。

【図3】 ディレクトリサービス・サーバの構成を示す図である。

11

【図４】 ディレクトリサービスデータベースの登録内容の説明図である。

【図５】 ディレクトリサービスデータベースを構成するオブジェクト情報テーブルの例を示す図である。

【図６】 ディレクトリサービスデータベースを構成するオブジェクトの属性情報テーブルの例を示す図である。

【図７】 従来のネットワークの問題点を説明するための図である。

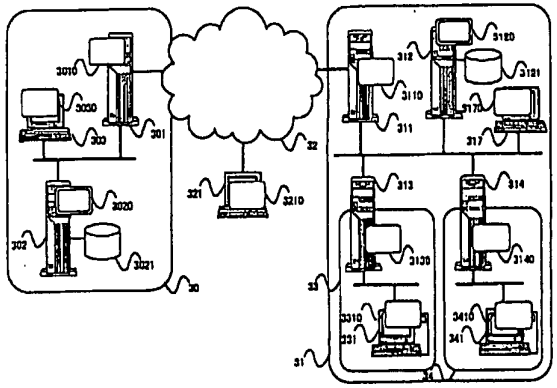
【図８】 従来のネットワークの別の問題点を説明するための図である。

【符号の説明】

10…A社ネットワークA、11…B社ネットワークB、101…クライアント計算機、102…ファイアウォール、103…ファイアウォール、110…B社サブネットワークC、111…ファイアウォール、112…ファイアウォール、20…社内ネットワーク、200…サブネットワーク、201…ファイアウォール、202…ファイアウォール、203…クライアント、204…設定コンソール、205…設定コンソール、30…ネットワーク、31…ネットワーク、32…インターネット、33…サブネットワーク、34…サブネットワーク、301…ファイアウォール、302…ディレクトリサービス・サーバ、303…クライアント、311…ファイアウォール、312…ディレクトリサービス・サーバ、313…ファイアウォール、314…ファイアウォール、317…クライアント、321…クライアント、331…サーバ計算機、341…サーバ計算機、3010…ファイアウォール兼中継サーバプログラム、3020…ディレクトリサーバプログラム、3030…中継サーバプログラム、3110…ファイアウォール兼中継サーバプログラム、3120…ディレクトリサーバプログラム、3130…ファイアウォール兼中継サーバプログラム、3140…ファイアウォール兼中継サーバプログラム、3210…中継サーバプログラム、3310…中継サーバプログラム、3410…中継サーバプログラム、41…ディスクコントローラ、42…主記憶装置、43…バス、44…CPU、45…通信I/Oインタフェースコントローラ、46…キーボードマウスコントローラ、461…キーボード、47…ビデオボードコントローラ、472…ディスプレイ装置、410…固定ディスク装置、411…通信プログラム、412…データ中継制御プログラム、413…ディレクトリ情報同期プログラム、414…中継経路テーブル、420…主記憶装置の内容、421…データ中継経路情報記憶領域、422…通信データ記憶領域、423…ディレクトリ同期情報記憶領域、424…プログラムロード領域、51…ディスクコントローラ、52…主記憶装置、53…バス、54…CPU、55…通信I/Oインタフェースコントローラ、56…キーボードマウスコントローラ、561…キーボード、57…ビデオボードコントローラ、572…ディスプレイ装置、510…固定ディスク装置、511…通信プログラム、512…ディレクトリデータベース制御プログラム、513…ディレクトリ情報同期プログラム、514…中継経路テーブルを含むディレクトリデータベース、520…主記憶装置の内容、521…ディレクトリデータ記憶領域、522…ディレクトリ同期情報記憶領域、523…プログラムロード領域、60…ディレクトリオブジェクト、61…ディレクトリオブジェクト、62…ディレクトリオブジェクト、63…ディレクトリオブジェクト、611…ディレクトリオブジェクト、612…ディレクトリオブジェクト、613…ディレクトリオブジェクト、621…ディレクトリオブジェクト、622…ディレクトリオブジェクト、623…ディレクトリオブジェクト、624…ディレクトリオブジェクト、625…ディレクトリオブジェクト、626…ディレクトリオブジェクト、70…ディレクトリオブジェクト情報テーブル、701…オブジェクトID、702…オブジェクト名、703…オブジェクトコンテキスト、704…オブジェクト型、705…オブジェクトの属性ID、710…オブジェクト情報、711…オブジェクト情報、712…オブジェクト情報、714…オブジェクト情報、715…オブジェクト情報、716…オブジェクト情報、717…オブジェクト情報、718…オブジェクト情報、719…オブジェクト情報、720…オブジェクト情報、721…オブジェクト情報、80…オブジェクト属性情報テーブル、801…属性ID、802…補助ID、803…オブジェクト属性名、804…オブジェクト属性シリアル、805…オブジェクト属性値、810…オブジェクト属性情報、811…オブジェクト属性情報、812…オブジェクト属性情報、813…オブジェクト属性情報、814…オブジェクト属性情報、815…オブジェクト属性情報、816…オブジェクト属性情報、817…オブジェクト属性情報、818…オブジェクト属性情報、819…オブジェクト属性情報、820…オブジェクト属性情報、821…オブジェクト属性情報、822…オブジェクト属性情報、823…オブジェクト属性情報、824…オブジェクト属性情報、825…オブジェクト属性情報、826…オブジェクト属性情報、827…オブジェクト属性情報、828…オブジェクト属性情報、829…オブジェクト属性情報、830…オブジェクト属性情報、831…オブジェクト属性情報、832…オブジェクト属性情報、833…オブジェクト属性情報。

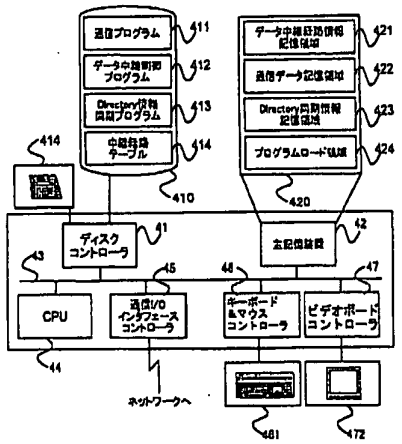
【図１】

図1



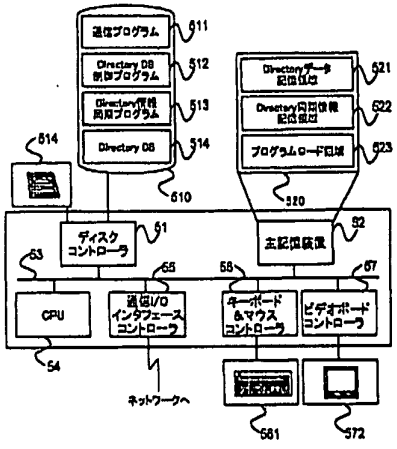
【図２】

図2



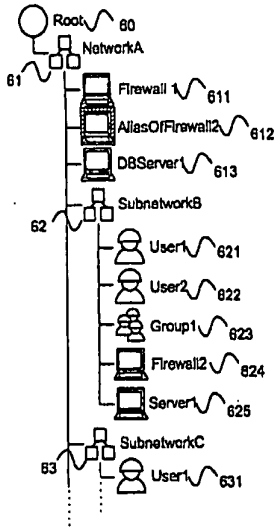
【図３】

図3



【図4】

図4



【図5】

図5

701 ObjID	702 Name	703 Context	704 Type	705 AttrID	
0000	Root	Root	Top	None	~710
0001	NetworkA	Root	Container	A0001	~711
0002	Firewall1	NetworkA.Root	Service	A0002	~712
0003	AliasOfFirewall2	NetworkA.Root	Alias	A0003	~713
0004	DBServer1	NetworkA.Root	Service	A0004	~714
0005	SubnetB	NetworkA.Root	Container	A0005	~715
0006	User1	SubnetB.NetworkA.Root	User	A0006	~716
0007	User2	SubnetB.NetworkA.Root	User	A0007	~717
0008	Group2	SubnetB.NetworkA.Root	Group	A0008	~718
0009	Firewall2	SubnetB.NetworkA.Root	Service	A0009	~719
0010	Server1	SubnetB.NetworkA.Root	Service	A0010	~720
:					
n	UserM	SubnetC.NetworkA.Root	User	A000n	~721

70

【図6】

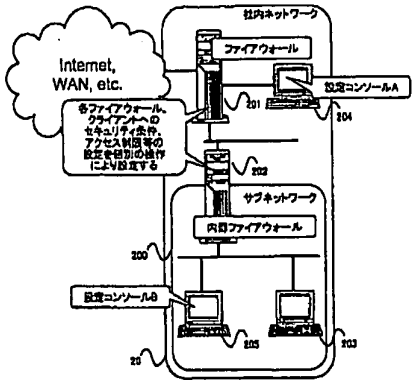
図6

801 AttrID	802 SubID	803 Name	804 Serial	805 Value	
A0001	0001	Owner	0	Supervisor	~810
:					
A0002	0001	Owner	0	Supervisor	~811
A0002	0002	AccessRight	0	User1=rw	~812
A0002	0003	AccessRight	1	User2=r	~813
A0002	0004	AccessRight	2	ProjectUser.External=r	~814
A0003	0001	Owner	0	Supervisor	~815
A0003	0002	OriginalEntity	0	Firewall2	~816
A0003	0003	AccessRight	0	User1=rw	~817
A0003	0004	AccessRight	1	User2=r	~818
A0003	0005	AccessRight	2	ProjectUser.External=r	~819
A0003	0006	AccessRight	3	Others=none	~820
A0004	0001	DBType	0	DirectoryService	~821
A0004	0002	AccessRight	0	User1=rw	~822
A0004	0003	AccessRight	1	User2=rw	~823
A0004	0004	AccessRight	2	ProjectUser.External=r	~824
A0004	0005	AccessRight	3	Others=none	~825
:					
A0009	0001	Owner	0	Supervisor	~825
A0009	0002	RoutePermission	1	User=All	~826
A0009	0003	RoutePermission	2	User2=Route.0	~827
A0009	0004	RoutePermission	3	ProjectUser.External=Route.0	~828
A0009	0005	RoutePermission	4	ProjectUser.External=Route.1	~829
A0009	0006	RoutePermission	5	Others=none	~830
A0009	0007	Route	0	DBServer1.Firewall1	~831
A0009	0008	Route	1	Server1.Firewall2.Firewall1	~832
A0010	0001	Owner	0	Supervisor	
:					
A000n	000p	Owner	0	Supervisor	~831

80

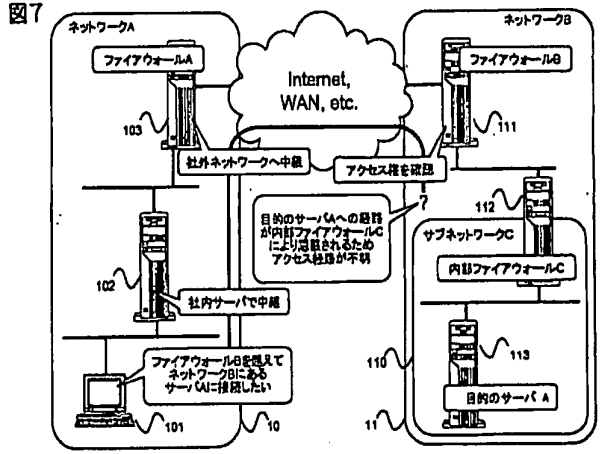
【図8】

図8



【図7】

図7



フロントページの続き

(72)発明者 萱島 信
神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 小泉 稔
神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 勝俣 修
神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア開発本部内